UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,216	03/10/2004	Steven M. Harris	3328.001	4133

30589 7590 01/05/2009

DUNLAP CODDING, P.C.
PO BOX 16370
OKLAHOMA CITY, OK 73113

EXAMINER	
SHAN, APRIL YING	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
01/05/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/797,216	HARRIS, STEVEN M.	
	Examiner	Art Unit	
	APRIL Y. SHAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-30* is/are pending in the application.

4a) Of the above claim(s) *5-19* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-4 and 20-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A Request for Continued Examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 20 October 2008 has been entered.

2. Claims 1, 4 and 20 have been amended. Claim 2 is canceled. Claims 5-19 are withdrawn from consideration due to Applicant's election without traverse to Election/Restriction Requirement dated August 24, 2007. No new claims have been added. Therefore, claims 1 and 3-30 are currently pending in the present application and claims 1, 3-4 and 20 -30 have been examined.

3. Applicant's amendments and argument have been fully considered, but are moot in view of new ground rejection as set forth below. It is noted that Applicant's arguments are directed towards limitations newly added via amendments. Any well known art statements made in the last Office Action that were not adequately and/or specifically traversed are taken as admittance of prior art as per MPEP 2144.03.

4. Any objection/rejection not repeated below is withdrawn due to

Applicant's amendment. More specifically, the examiner withdraws the pending 35 USC § 101 rejection to claims 20 - 30 after careful reviewing Applicant's amendment and remark (pages 14-16). The examiner acknowledges that "The computer readable medium is capable of storing the logic…Common examples of computer readable mediums include hard disks, optical disks, floppy disks, tapes, memory, or the like", which is disclosed in the paragraph [0023] of the original disclosure and cited by the Applicant in the remark. Therefore, the computer readable medium in the instant application does not include signal or carrier wave and claims 20-30 are statutory.

5. The examiner acknowledges amendments made to paragraph [0031] of the instant specification and no new matter is introduced.

Claim Objections

6. Claims 20-30 are objected to because of the following informalities:

Claim 20 recites, "An unlocking program stored on a computer readable medium **for** unlocking a password protected content file stored on a computer readable medium". Such a recitation may be interpreted as merely an intended use for the unlocking program. Examiner suggests replacing "for unlocking" with "to unlock" in order to more positively recite, "An unlocking program stored on a computer readable medium to unlock", thereby the claim language is not merely

a possible intended use for the unlocking program stored on a computer readable medium.

Claims 21- 22 and 24 - 27 recite "The unlocking program…for initiating...for causing...for preventing...for monitoring...for automatically terminating..." which have similar deficiencies as claim 20.

Any claim not specifically addressed, above, is being objected as incorporating the deficiencies of a claim upon which it depends.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. **Claims 1, 4 and 20-21** are rejected under 35 U.S.C. 103(a) as being unpatentable over Graunke et al. (*U.S. Patent No. 5,991,399*) in view of Vestergaard et al. (*U.S. Patent No. 7,466,823*).

As per **Claim 1**, Graunke et al. discloses:

distributing to the recipient's computer an unlocking program having a password embedded within the unlocking program, the password corresponding to the password protecting the content file *(Tamper resistant key module 52 containing the necessary key (i.e. one symmetric key) to decrypt the content is forwarded over communication network 34 to client 32 – e.g. col. 7, lines 16 - 58 and Fig. 2. Please note tamper resistant key module containing the necessary key to decrypt the content corresponds to Applicant's unlocking program having a password embedded within the unlocking program and client corresponds to Applicant's recipient's computer*);

distributing the password protected content file to the recipient's computer (*The encrypted digital content 36 downloaded over communication network 34 via line 40 to client 32 and the encrypted content is not accessible without a key to decrypt it – e.g. col. 6, lines 17- 35, abstract and Fig. 2. Please note the encrypted content is not accessible without a key corresponds to Applicant's the password protected content file*) wherein the unlocking program automatically supplies the password embedded within the unlocking program to an application program upon the application program loading the password protected content file wherein the password embedded within the unlocking program (*The trusted*

player uses the private key wrapped into an executable tamper resistant key module to decrypt encrypted digital content - e.g. abstract and col. 8, line 61 – col. 9, line 1. Please note trusted player corresponds to Applicant's application program).

Although Graunke et al. disclose *tamper resistant key module 52 containing the necessary key is resistant to observation and modification to an attacker (e.g. col. 5, lines 52-55),* Graunke et al. does not explicitly disclose the password is not revealed to the recipient, however, Vestergaard et al. met the claimed limitation by disclosing *the consumer never comes into direct contact with a decryption key, as the issuance and installation of a decryption key is done automatically and transparently to the user. Keys are issued between the MPE player and MPE servers without exposing them to the Consumer 130 (e.g. col. 14, lines 32 – 37).*

Graunke et al. - Vestergaard et al. are analogous art because they are from a similar field of endeavor in secure distribution of digital content over computer networks (i.e. Internet). Thus, it would have been obvious to a person with ordinary skill in the art, at the time of invention, to modify the teachings of Graunke et al. with the password (i.e. decryption key) is not revealed to the recipient taught by Vestergaard et al. The motivation for doing so would have been to provide a simple but powerful security solution that benefit content owners, content distributors *(e.g. Vestergaard et al., col. 14, lines 6 -12 and 43 - 46)*.

As per **Claim 4**, Graunke et al. - Vestergaard et al. discloses a method as applied above in claim 1. Graunke et al. - Vestergaard et al. further discloses wherein steps a and b are repeated at a predetermined rate and wherein the password protecting the content file and the password accessed by the unlocking

program are different in each repeat cycle (*Graunke et al., the private key is dynamically generated, associated with specific digital content, communicated in real-time and the encrypted content may be a file downloaded over communication network prior to usage – e.g. abstract, col. 3, line 67 – col. 4, line 1; Vestergaard et al., in Step E, the consumer 130 may downloaded MPE file and in Step H, the MPE servers send a copy of the Song Key to the MPE player to decrypt the song – e.g. col. 7, line 55 – col. 8*, line 45, *presented as loops to either download a new MPE file or exit – e.g. col. 9, lines 4-11 and the decryption key of each song is called a song key - e.g. col. 14, lines 38 - 41. Please note in the Vestergaard et al. reference, each song key is inherently different in each repeat cycle since a new file (i.e. new song) is downloaded in each repeat cycle).*

As per **Claim 20**, Graunke et al. - Vestergaard et al. discloses the claimed method of steps as applied above in claim 1. Claim 20 contains subject matter similar to claim 1, and thus, Graunke et al. - Vestergaard et al. discloses the unlocking program stored on a computer readable medium for unlocking a password content file.

As per **Claim 21**, Graunke et al. - Vestergaard et al. discloses an unlocking program as applied above in claim 20. Graunke et al. et al. further discloses wherein the unlocking program includes at least one instruction for

initiating the application program and for causing the application program to load the content file *(the key module checks the integrity and authenticity of the trusted player and if the trusted player is validate, the key module uses a symmetric key to decrypt the encrypted content. The trusted player then plays the newly decrypted content for the user – e.g. col. 8, line 43 – col. 9, line 16)*

10. **Claims 3 and 23** are rejected under 35 U.S.C. 103(a) as being unpatentable over Graunke et al. (*U.S. Patent No. 5,991,399*) in view of Vestergaard et al. (*U.S. Patent No. 7,466,823*) and further in view of Pace et al. (*U.S. Patent No. 6,460,050*).

As per **Claims 3 and 23**, Graunke et al. - Vestergaard et al. discloses a method/unlocking program as applied above in claims 1 and 20. Graunke et al. further disclose monitor the application program for a request for a password (*e.g. col. 9, lines 1-16*). Although Graunke et al. mentions unlocking program is an executable tamper resistant key module (*e.g. abstract*) and decryption key must be dynamically provided to the trusted software and not pre-loaded *(e.g. col. 2, lines 62-64)*, Graunke et al. - Vestergaard et al. does not explicitly disclose the program is adapted to run separately/independently from the application program. Pace et al., however, discloses that *an executable may be run as a separate process from a host application (i.e. a first tier system) (e.g. col. 4, line*

15), which met the claimed limitation of the program is adapted to run separately/independently from the application program.

Graunke et al. - Vestergaard et al. - Pace et al. are analogous art because they are from a similar field of endeavor in content transfer in a client-server computing environment via networks (i.e. Internet). Thus, it would have been obvious to a person of ordinary skill in the art, at the time of invention, to modify the teachings of Graunke et al. - Vestergaard et al. with an executable may be run as a separate process from a host application taught by Pace et al. in order to work as a standalone executable to be dynamically updated and not pre-loaded into the host application.

This combination would predictably result a well known standalone executable to be dynamically updated and not pre-loaded into the host application, thus providing one way of enabling decryption keys embedded in the executable to be dynamically updated and not pre-loaded as required by Graunke et al. It has been held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does not more than yield predictable results." *KSR.*, 127 S. Ct. at 1739, 82USPQ2d at 1395 (2007) (citing *Graham*, 383 U.S. at 12).

11. **Claim 22** is rejected under 35 U.S.C. 103(a) as being unpatentable over Graunke et al. (*U.S. Patent No. 5,991,399*) in view of Vestergaard et al. (*U.S. Patent No. 7,466,823*) and further in view of Schreiber et al. *(U.S. Patent No. 6,298,446)*.

As per **Claim 22**, Graunke et al. - Vestergaard et al. discloses the unlocking program, as applied to claim 20, but does not explicitly disclose includes means for preventing a screen capture representing at least a portion of the content stored in the password content file, however, Schreiber et al. discloses *SafeMedia includes enhanced system control for preventing screen capture by disabling a clipboard (e.g. col. 2, lines 27-30).*

Graunke et al. - Vestergaard et al. - Schreiber et al. are analogous art because they are from a similar field of endeavor in digital content distribution over a network. Thus, it would have been obvious to a person of ordinary skill in the art, at the time of invention, to modify the teachings of Graunke et al. - Vestergaard et al. with preventing screen capture by disabling a clipboard taught by Schreiber et al. The motivation of doing so would have been to provide enhanced system control to protect software from rampant unauthorized copying, distribution and use *(e.g. Schreiber et al., col. 1, lines 21-23 and col. 2, lines 27-30).*

12. **Claim 24-29** are rejected under 35 U.S.C. 103(a) as being unpatentable over Graunke et al. (*U.S. Patent No. 5,991,399*) in view of Vestergaard et al. (*U.S. Patent No. 7,466,823*) and further in view of Winneg et al. (U.S. Patent No. 7,069,586).

As per **Claims 24 -26 and 28- 29**, Graunke et al. - Vestergaard et al. discloses an unlocking program as applied above in claim 20. Although Graunke

et al. - Vestergaard et al. discloses a person computer (PC) platform computing system *(Graunke et al., e.g. Fig. 2 and col. 4, lines 24 – 2 7 and Vestergaard et al., e.g. col. 4, lines 10-14),* Graunke et al. - Vestergaard et al. does not explicitly disclose monitoring the running of at least one system administration program (i.e. Task Manager program) capable of terminating the program and automatically terminating the system administration program/the application program upon detecting the running of such system administration program and to prevent termination of a program. However, Winneg et al. discloses: *the unauthorized process list may include browser applications, applications for scheduling tasks to be performed on the computer system, and applications for managing tasks performed on the computer system, (e.g., Microsoft Task Manager). Terminating task-managing manager and task-scheduling applications prevents a process (e.g., an application) that has been scheduled to execute during execution of the first application from executing (e.g. col. 19, lines 46 -60),* which met the claimed limitation of monitoring the running of at least one system administration program (i.e. Task Manager program) capable of terminating the program and automatically terminating the system administration program/the application program upon detecting the running of such system administration program and to prevent termination of a program.

Graunke et al. - Vestergaard et al. - Winneg et al. are analogous art because they are from a similar field of endeavor in a person computer (PC) platform computing system. Thus, it would have been obvious to a person of

ordinary skill in the art, at the time of invention, to modify the teachings of Graunke et al. - Vestergaard et al. with monitoring the running of at least one system administration program (i.e. Task Manager program) capable of terminating the program and automatically terminating the system administration program/the application program upon detecting the running of such system administration program and to prevent termination of a program taught by Winneg et al. in order to provide information about the processes and programs running on a computer, as well as the general status of the computer and also to ensure unauthorized content may not be accessed *(e.g. Winneg et al., col. 2, lines 38-39 and col. 19, lines 46 -60)*

This combination would predictably result a well known computing system includes/terminates a Task Manager program provided with a Windows operating system to provide general status of a computer and ensure application security. It has been held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does not more than yield predictable results." *KSR.*, 127 S. Ct. at 1739, 82USPQ2d at 1395 (2007) (citing *Graham*, 383 U.S. at 12).

As per **Claim 27,** Graunke et al. further discloses wherein the unlocking program includes an instruction for terminating the unlocking program after the application program has been terminated (*plug-in, which would inherently be*

terminated after host application program (i.e. application program) was terminated – e.g. col. 7, lines 42 -43).

13. **Claim 30** is rejected under 35 U.S.C. 103(a) as being unpatentable over Graunke et al. (*U.S. Patent No. 5,991,399*) in view of Vestergaard et al. (*U.S. Patent No. 7,466,823*) and further in view of Rodgers et al. (*U.S. Patent No. 7,210,039*).

As per **Claim 30**, Graunke et al. - Vestergaard et al. discloses the unlocking program, as applied to Claim 20, but does not explicitly teach wherein the file is characterize as a .pdf file, however, Rodgers et al. discloses *the digital content may be a PDF file (e.g. col. 3, lines 56 - 57 and col. 11, lines 41 – 45)*, which met the claimed limitation of wherein the file is characterize as a .pdf file.

Graunke et al. - Vestergaard et al. - Rodgers et al. are analogous art because they are from a similar field of endeavor in secure digital content distribution. Thus, it would have been obvious to a person of ordinary skill in the art, at the time of invention, to modify the teachings of Graunke et al. - Vestergaard et al. with the file is characterize as a .pdf file taught by Pace et al. in order to be in compliance with an industry standard for printable documents on the Web.

This combination would predictably result a well known format in compliance with an industry standard for printable documents on the Web. It has been held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does not more than yield predictable

results." *KSR.*, 127 S. Ct. at 1739, 82USPQ2d at 1395 (2007) (citing *Graham*, 383 U.S. at 12).

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. However, applicants are **strongly urged** to consider the cited references carefully and distinguish them from the instant claims in accordance with 37CFR 1.111c when presenting an amendment in response to the current Office Action.

- Byrne (U.S. Patent No. 6,223,288) discloses secure network-based distribution of protected and unprotected data
- Riebe et al. (U.S. Patent No. 7,200,760) discloses a user must obtain a license key in order to decrypt the critical data elements before the software program can be used
- Hatanaka et al. (U.S. Patent No. 7,203,312) discloses a cellular phone has distributed encrypted content data and uses a content key to decrypt the encrypted content
- Wang (U.S. Patent No. 7,356,688) discloses transferring among key holders in encoding and cryptographic systems the right to decode and decrypt messages in a way that does not explicitly reveal decoding and decryption keys

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to APRIL Y. SHAN whose telephone number is (571)270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/April Y Shan/
Examiner, Art Unit 2435